ISSN No. 0976-5697

Volume 6, No. 1, Jan-Feb 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Possible security related threats to the Student Information Management System and its solution

Aditya A. Shastri
M. Tech Scholar
Computer Science and Engineering
Government College of Engineering
Amravati, India

Dr. P. N. Chatur
Head of Dept.
Computer Science and Engineering
Government College of Engineering
Amravati, India

Prof. R. V. Mante
Asst. Prof
Computer Science and Engineering
Government College of Engineering
Amravati, India

Abstract: The Student Information Management System (SIMS) is a student-level data collection system that allows the college, university or any other organization to collect and analyse more accurate and comprehensive information related to students. Data related to students are stored in repositories like database or data warehouse. As this data is very important it is essential to make arrangements about the security of database. This database contains important data of students and also confidential matters about college or university. This paper propose several possible threats to the student information system and also gives the model that can be used to improve the security of the system.

Keywords: Database Security; Database Attacks; SIMS; Security enhanced module; Safety rule base; optimization.

I. INTRODUCTION

The student information management system is the software used for educational purpose by the schools, colleges, universities or even offices who require to maintain data regarding their employees. The Student Information Management System (often called as SMIS) provides graphical user interface for entering the marks of students, teacher's assessments, keep record of student attendance and manage other student related data. We can consider SMIS equivalent to the ERP system (Enterprise Resource Planning) for corporate customers.[1] Some of the important functions that this system perform are handling admission process, enrolling new student, handling records of examinations, assessments, grades, academic progression, GPA, maintaining discipline records, communicating student details to parent through parent portal, maintaining records about students attendance and absentees, maintaining student behavior, schemes about set of subjects offered to different, student health record, canteen management, fees management, payroll processing for the staffs etc.[2]

In past many colleges and universities have created their own student record system. One such example is ROSI system (Repository of Student Information) at University of Toronto. [3] But with the growing complexities of the system, most organization choose to buy customizable software.

A. Overview:

Student Information Management System contains important data. So security of this data is of uttermost importance. In this paper, all possible threats to the security of database are mentioned and a model is proposed which can be used for increasing the security.

B. Sources of threats to database:

Security related threats can origin from following three main types or even from the combination of the following sources.

a. Internal Threats: These are the threats that originates from within the organization. This includes the human assets like employees, interns and organization executives. Most people from within the organization are trusted to only certain degree and some like professors can have high degree of privileges.[4]

b. External Threats: These are the threats that originate from the sources that are outside the organization. For example this include hackers, organized crime group, government entities as well as environmental events. Typically, no privileges or access level is provided for these types of people.[4], [5]

c. Partner Threats: This include any third party sharing a business relationship with the organization. This value chain of partners, vendors, suppliers, contractors, customers is known as the extended enterprise. Information exchange is the necessary for the extended enterprise and, for this reason, some level of trust and privilege is usually implied between business partners.[4]

In this paper we mainly concern about security arising from internal threats. So a model is proposed which will help to increase the security of database from internal threats.

II. PROPOSED SYSTEM DEVELOPMENT

In this section we will study the existing system as well as proposed system along with their architecture.

A. Existing System:

Presently database can be accessed by establishing connection between client and database server through programming technologies like Java, .net etc. Just a one line connection string is required to establish a connection. So the existing system looks as shown in Fig. 1. [6], [7]

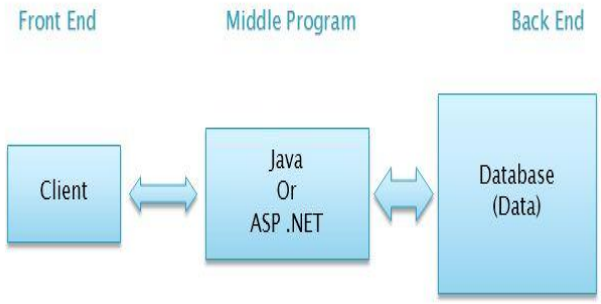

Figure. 1 Existing SIMS Architecture

Here in this system architecture there is no measure for security of database. [8] Once the connection is established, any user will be able to access any information from any table in database.

B. Proposed System:

As you have seen in the existing system architecture, there is no measure of security. So for this purpose we will introduce a model that will check for the security of database from internal threats. So the proposed system architecture becomes as shown in Fig. 2.

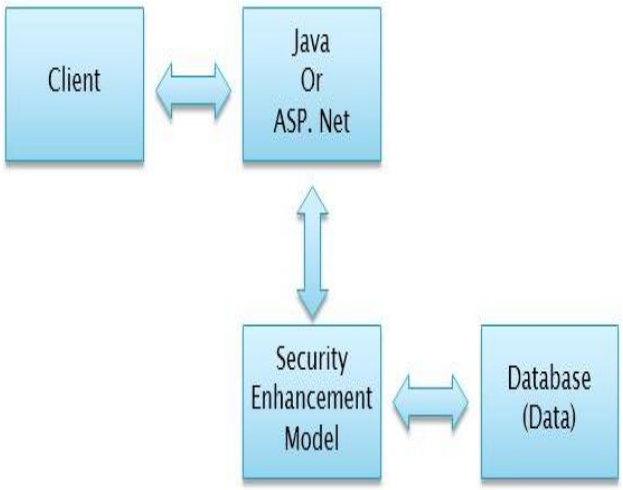

Figure. 2 Proposed System Architecture

Security enhancement model is used to increase the security of database. This model is introduced between client end and database server end.

C. Security Enhancement Model:

Security enhancement module consist of two parts. They are as follows.

a. Agent Module: The main function of the agent module is that according to the result of the security detect module it performs access filter. And then generate the safety response according to which query fired by user is executed.

b. Security detect module: The main function of the security detect module is that it checks whether particular user is accessing only those parts of database to which he is having the access. Also whether he is performing only those operation which are allowed to that user by Database Administrator (DBA). For this it takes help from safety rules defined by Database Administrator for each users.[9] This safety rule maintains set of operation that the user can perform on particular set tables.

III. WORKING OF SECURITY ENHANCEMENT MODEL

Initially user will fire a query. This query will be transferred to Access Filter module which filters the query that is it detects the type of query whether select, update, delete etc. This filter will also determine the table on which the user wants to perform the operation. The results from this module is transferred to safety detect module of security detect model as shown in Fig. 3. It is the function of this module to check for the security of system. It takes help from security rule base. As already discussed security rule base is maintained by Database Administrator. This part of database is solely operated by DBA. According to the safety detect module and security rule base, a security response is generated which is transferred back to the agent model. Again with the help of this safety response, agent module decides whether to allow the user to access the part of database which he wants to access or not.

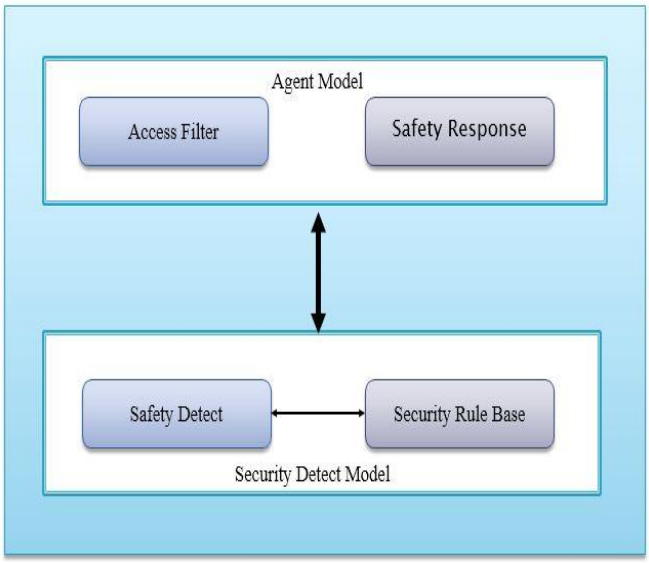

Figure. 3 Security Enhancement Model Architecture.

If safety response is false then user is not allowed to perform the operation on that part of database on which he wants to and if it is true then he is allowed to access the table.

IV. CONCLUSION

Database system is the core component of many computing system. In this paper we have discussed various threats to the database system and we mainly focused on internal threats. A model is proposed to improve the security

of the database from internal threats. This model is introduced between the client and the database server end. The addition of the security enhancement model increased the security of database but it also increase the response time of the overall system. If we use the database optimization, the performance and the safety of the database can be upgraded.

V. REFERENCES

[1] Peng Wang, Liu Xing, Xin Gu, Changming Zhu "Design and Implementation of Security Enhanced Module in Database" 978-0-7695-5118-0/13 © 2013 IEEE DOI 10.1109/ICICSE.2013.20

[2] Yi Huang, Xinqiang Ma "A Security Model Based on Database System" 978-0-7695-4031-3/10 © 2010 IEEE DOI 10.1109/iCECE.2010.1198

[3] Zhu Yangqing, Yu Hui, Li Hua "Design of A New Web Database Security Model" 978-0-7695-3643-9/09 © 2009 IEEE DOI 10.1109/ISECS.2009.180

[4] Nedhal A. Al-Sayid, Dana Aldlaeen "Database Security Threats: A Survey Study" 978-1-4673-5825-5/13 ©2013 IEEE.

[5] Raymond Chiong and Sandeep Dhakal "Modelling Database Security through Agent-based Simulation" 978-0-7695-3136-6/08 © 2008 IEEE DOI 10.1109/AMS.2008.164

[6] Xueyong Zhu, J. William Atwood "A Web Database Security Model Using the Host Identity Protocol" 11th International Database Engineering and Applications Symposium (IDEAS 2007) 0-7695-2947-X/07 © 2007

[7] WANG Baohua, MA Xinqiang, LI Danning "A Formal Multilevel Database Security Model" 978-0-7695-3508-1/08 © 2008 IEEE DOI 10.1109/CIS.2008.45

[8] Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE "Database Security—Concepts, Approaches, and Challenges" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2005

[9] Premchand B. Ambhore,B.B.Meshram,V.B.Waghmare "A IMPLEMENTATION OF OBJECT ORIENTED DATABASE SECURITY" Fifth International Conference on Software Engineering Research, Management and Applications 0-7695-2867-8/07 © 2007 IEEE DOI 10.1109/SERA.2007.120 359